



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,337	01/27/2004	Derek L. Davis	42P6514C	3287
<div>7590 04/06/2007 Blakely, Sokoloff, Taylor & Zafman LLP 7th Floor 12400 Wilshire Boulevard Los Angeles, CA 90025</div>			<div>EXAMINER FIELDS, COURTNEY D</div>	
			ART UNIT	PAPER NUMBER
			2137	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		04/06/2007	PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/766,337	DAVIS DEREK L.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-11 and 13-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-11 and 13-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>27 January 2004</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1,12 and 20-21 have been cancelled.
2. Claims 2,13,15, and18 have been amended.
3. Claims 2-11 and 13-19 are pending.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2-11 and 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel U.S. Patent No. 6,327,660 in view of Krawczyk, Hugo "New Hash Functions for Message Authentication".

As per claim 2, Patel discloses a method for securing communications between a first device and a second device comprising: a processing unit /main memory (first device) coupled together by a chipset and a system resource comprising a storage device which includes a non-volatile memory (flash memory) (second device) communicating over a communication channel. A bus provides a pathway between the processing unit and/or memory, and one or more system resources in Column 3, lines 41-67. The BIOS code within the memory can be used as a means for "challenge/response" protocol in Column 4, lines 1-9. The booting process as described in Patel is used as means for mutual authentication between the first and second device, in which layered software comprising a communication application, security

communication protocol, key manger, etc. is used to secure communications between the two devices in Column 4, lines 10-27. Patel discloses if first electronic device needs to communicate with the second device, security association and/or keying material is stored within the flash memory of the system resource (second device) in Column 6, lines 59-67, Column 7, lines 1-20. Patel also discloses IKE defined as a protocol used for system authentication used to generate keys using Diffie-Hellman exchange (digital signatures) and protecting communications between the devices in Column 7, lines 54-67. Patel also discloses within the processing unit (first device), an integrity check value is performed through the use of IPSEC AH. This protocol is designed to protect the integrity of information transmitted between electronic systems in Column 4, lines 29-67, Column 5, lines 1-21.

However, Patel does not explicitly disclose the feature of extracting bits from a pseudo-random data stream for use in a matrix having M rows and N columns.

Krawczyk teaches a method and system which uses Toeplitz matrices.

Krawczyk discloses the claimed limitation of extracting bits randomly for use as coefficients of a matrix having M rows and N columns and performing operations to generate the integrity check value. (See pages 301-303)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-

Art Unit: 2137

random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 3, (Patel as modified by Krawczyk) discloses the claimed limitation of inputting keying material into a cipher engine performing operations in accordance with a stream cipher and producing the pseudo-random stream by the cipher engine. (See Krawczyk, page 302)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 4, (Patel as modified by Krawczyk) discloses the claimed limitation wherein a counter mode stream cipher in Data Encryption Standard. (See Krawczyk, page 304, Section 2.2, 1st and 2nd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person

having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 5 and 9, (Patel as modified by Krawczyk) discloses the claimed limitation of assigning M bits from the selected number of bits as a first column of the matrix and assigning M bits for each remaining column of the matrix. (See Krawczyk, page 307)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 6 and 10, (Patel as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on M bits from the content of the message and coefficients of the first column of the matrix and performing an exclusive OR operation between each of the values to produce integrity check value. (See Krawczyk, page 304, Section 2.2, 1st paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 7, (Patel as modified by Krawczyk) discloses the claimed limitation wherein the arithmetic operations are bitwise multiplication operations. (See Krawczyk, page 304, Theorem 3, and 3rd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 8, (Patel as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on the M bits from the message for a N-1 column of the matrix and performing exclusive OR operations between values associated with N-1

Art Unit: 2137

column of the matrix to produce $N-1$ bits of the integrity check value. (See Krawczyk, page 307, Section 3)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 11 and 17, (Patel as modified by Krawczyk) discloses the claimed limitation of computing the integrity check value based on bits in the message, and determining if the bits differ from the predetermined bits set for the integrity check value. (See Krawczyk, page 309)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 13, (Patel as modified by Krawczyk) discloses the claimed limitation of computing an integrity check value for an incoming message and determining whether the incoming message is valid by comparing the computed integrity check value with the recovered integrity check value (See Column 5, lines 15-21, Column 6, lines 1-15) and decrypting the incoming message before an integrity check is performed. (See Krawczyk, page 307, Section 3.1)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 14, 15, and 16, (Patel as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on M bits from the content of the message and coefficients of the first column of the matrix and performing an exclusive OR operation between each of the values to produce integrity check value. (See Krawczyk, page 304, 1st and 2nd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification

Art Unit: 2137

would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 18, (Patel as modified by Krawczyk) discloses the claimed limitation the first device includes a integrity check value generator to produce an integrity check value based on a selected group of its from a pseudo-random data stream and contents of the message. (See Krawczyk, page 308, Section 4 and page 309, 1st and 2nd paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See page 30 - Introduction)

As per claim 19, (Patel as modified by Krawczyk) discloses the claimed limitation wherein the first device is a processor and the second device is a memory. (See Patel, Column 3, lines 45-47)

Art Unit: 2137

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Patel's securing communication method by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See page 30 - Introduction)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.


cdf

March 30, 2007


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER